

Windows Update & Defender

Schouder het geweer!

Microsoft gaat er prat op dat Windows met Vista alweer een stuk veiliger is geworden. Dat klopt ook wel, maar veel hangt toch af van hoe jij met die beveiliging omspringt! In deze workshop optimaliseren we alvast Windows Update en Windows Defender. TOON VAN DAELE

WAT DOEN WE?
- JE SYSTEEM BEVEILIGEN

WAARMEE?
- WINDOWS UPDATE, WINDOWS DEFENDER (EN EVENTUEEL EXTERNE ANTIVIRUSTOOL)

HOELANG?
- 30 MINUTEN

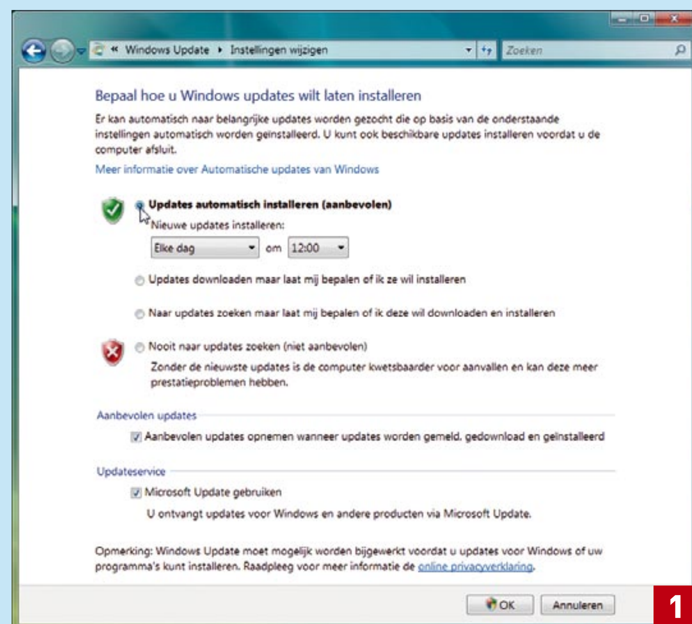
MOEILIJKHEID?



Microsoft heeft met Vista op diverse niveaus aan de veiligheid gesleuteld. Zo is er het nieuwe gebruikersaccountbeheer, waarmee malafide software minder speelruimte op je systeem moet krijgen. Niet onbelangrijk is ook de verbeterde firewall van Vista, en die krijgt alle aandacht in deel 10 van deze reeks. In deel 8 hadden we het uitgebreid over de module voor Ouderlijk toezicht. In deze negende aflevering concentreren we ons echter op de vernieuwde Windows Update – jawel, ook een belangrijke poot aan de beveiligingsstrategie van Vista – en vooral op Microsofts spionnenjager: Windows Defender. In ons kaderstukje ten slotte verneem je meer over antivirussoftware voor Vista.

STAP 1 / WINDOWS UPDATE CONFIGUREREN

Windows Update ken je natuurlijk al van vroegere Windows-versies. Het is een service van Microsoft die zorgt dat je Windows up-to-date blijft – ook naar beveiligingsupdates en patches toe. In Vista is deze dienst echter een heuse toepassing geworden, die je via de klassieke weergave van het **Configuratiescherm** of vanuit het Vista-startmenu kan opstarten. Het bovenste deel van het dialoogvenster deelt je de huidige status mee en wijst je op eventuele acties die je moet ondernemen, zoals het installeren van updates. Nu kan je natuurlijk op geregelde tijdstippen dit dialoogvenster openen en beschikbare updates downloaden en installeren, maar het is alleszins makkelijker én veiliger als je Windows dat klusje laat klaren. Klik op de knop **Instellingen wijzigen** en zet bij voorkeur een vinkje naast **Updates automatisch installeren**, waarbij je een geschikte frequentie en tijdstip instelt – standaard is dat **Elke dag om 3.00 uur** (zie afbeelding 1). Als je een vinkje plaatst bij **Aanbevolen updates opnemen wanneer [...]**, dan worden bij deze automatische updates niet alleen de essentiële updates (met name beveiligingspatches) maar ook aanbevolen updates (zoals nieuwere versies van gesigneerde stuurprogramma's) mee opgenomen. Bevestig met **OK** en met **Doorgaan**.



Automatische updates: makkelijk en veilig.

STAP 2 / WINDOWS UPDATE VERKENNEN

Terug in het hoofdvenster van Windows Update zie je onderaan de link **Updates voor andere producten downloaden**. Als je deze link aanklikt, beland je op een webpagina van Windows Update. Hier kan je dan aangeven dat je inderdaad ook updates voor andere Microsoft-producten – waaronder Office – mee met de automatische updates wil laten installeren. Na je fiat zal je merken dat de link in het dialoogvenster is vervangen door de melding **U ontvangt updates: Voor Windows en andere producten via Microsoft Update** (zie afbeelding 2). Alweer een zorg minder. Als je in de vorige stap had geopteerd voor **Naar updates zoeken maar laat mij bepalen of ik deze wil downloaden en installeren**, dan kan het gebeuren dat je een of andere

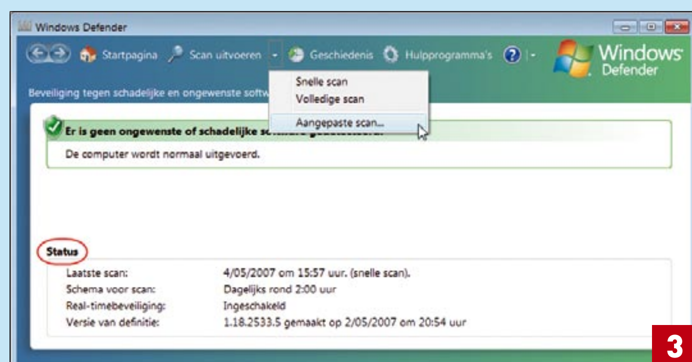


Ook optionele updates laten zich vanuit dit venster binnenhalen.

update liever niet accepteert. Windows blijft je dan echter bestoken met de vraag of je die update echt niet wil. Dat kan je gelukkig voorkomen. Klik op de link **Beschikbare updates** weergeven, klik met de rechtermuisknop op de gewraakte update en kies **Update verbergen**. Bevestig met **Doorgaan**. Keer je op je beslissing terug? Selecteer dan **Verborgen updates herstellen** in het linker taakpaneel, stip de bewuste update aan en druk op de knop **Herstellen**. Ondervind je onverhoeds problemen met een update, en wil je die liever weer kwijt? Klik dan onderaan het taakpaneel op **Geïnstalleerde updates**. Ga na of de bewuste update in de lijst verschijnt. Zo ja, selecteer die dan en druk op de knop **Verwijderen**.

STAP 3 / WINDOWS DEFENDER OPSTARTEN

Een antivirusprogramma heeft het natuurlijk vooral op virusachtigen gemunt. *Malware* ontsnapt echter vaak aan zo'n virusscan. Precies daarom zit in Vista een heuse spionnenjager ingebouwd: Windows Defender. Overigens kan je dit programma ook wel zelf downloaden en bijvoorbeeld onder Windows XP laten draaien (zoek naar Windows Defender op www.microsoft.com/downloads). Je roept de tool onder Vista op vanuit het startmenu – het volstaat om *defender* in te tikken in de zoekbalk. Meteen beland je in het hoofdvenster, waar je onderaan de status van de beveiliging afleest (zie afbeelding 3). Er is echter ook ruimte om zelf het heft in handen te nemen...



Standaard is Defender ingeschakeld voor real-time beveiliging en automatische scans.

STAP 4 / WINDOWS DEFENDER CONFIGUREREN

Zo kan je perfect instellen hoe vaak, wanneer en hoe grondig Defender z'n werk moet doen. Druk daarvoor op **Hulpprogramma's** en kies **Opties**. Laat bij voorkeur het vinkje staan bij **Scan automatisch op computer uitvoeren**, en kies een geschikte frequentie en tijdstip (standaard is dat **Dagelijks om 2:00 uur**). Voor een automatische scan laat je het type best ingesteld op **Snelle scan**, waarbij enkel die locaties worden gecontroleerd die gegeerd zijn door spionnen (zie stap 5 voor een volledige scan). De overige instellingen zijn standaard prima ingesteld, en hoef je dus niet te wijzigen. We raden je alvast aan het vinkje naast **Real-timebeveiliging gebruiken** te laten staan (zie afbeelding 4). Windows Defender zal je dan een waarschuwing geven zodra malware zich op de computer tracht te installeren of zichzelf probeert uit te voeren (zie ook stap 6). Valt Defender je bij elke scanronde lastig met de melding dat een bepaald programma mogelijk malware is – terwijl je de toepassing vertrouwt – dan kan je bij **Geavanceerde opties** via de knop **Toevoegen** dit programmabestand als uitzondering laten opnemen. Mocht je om een of andere reden toch Defender willen uitschakelen, verwijder dan het vinkje naast **Windows Defender gebruiken**. Bevestig je keuzes met **Opslaan** en met **Doorgaan**.

VISTA-WORKSHOPS

Nu het nieuwe besturingssysteem van Microsoft in de winkel ligt, zijn we gestart met een gloednieuwe 12-delige reeks workshops over Vista. Hieronder vind je alvast een overzicht.

1. INSTALLEREN
Zet Vista naast XP

2. VERKENNEN
De nieuwe interface uitgepluisd

3. AGENDA
Afspraken en taken plannen

4. FOTOGALERIJ
Foto's beheren & bewerken

5. MEDIACENTER
Multimedia op pc én tv

6. DVD MAKER
Films maken en branden

7. BACK-UPCENTRUM
Bestanden veiligstellen

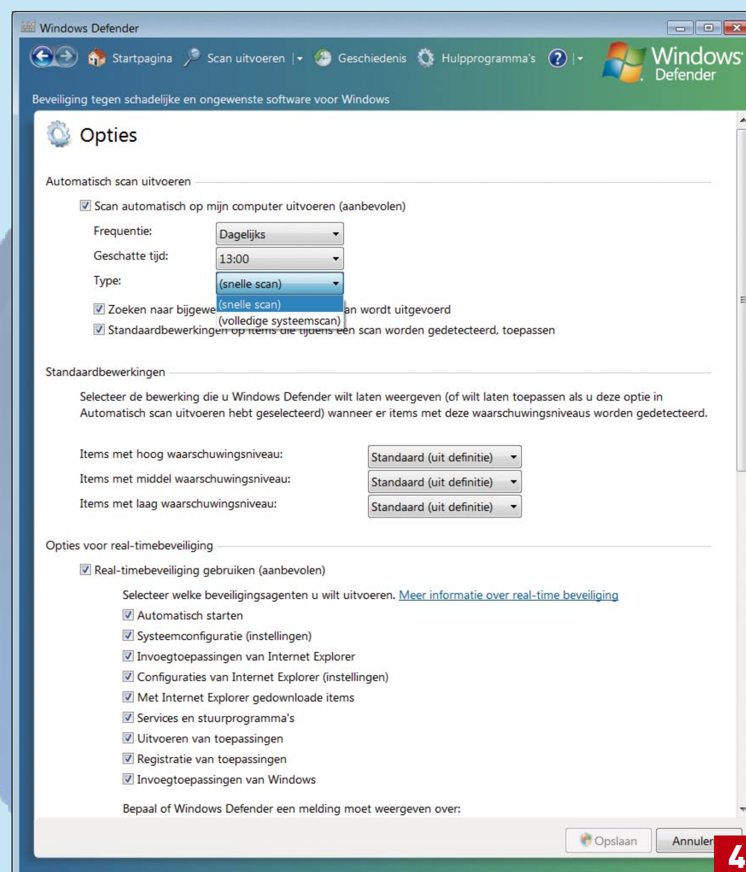
8. OUDERLIJK TOEZICHT
Computergebruik aan banden

9. BEVEILIGING
Internetbedreigingen buiten!

10. NETWERKEN
Thuisnetwerkje opzetten

11. FIREWALL
Internetverkeer regelen

12. PROBLEEMOPLOSSING
Diagnose en oplossingen



Defender zet verschillende 'agenten' in voor real-time beveiliging.



GEEN SPYWARE MEER

STAP 5 / MANUEEL SCANNEN

Krijg je op een bepaald moment het vermoeden dat malware zich toch in je systeem heeft weten te nestelen, dan is een grondiger scanronde aangewezen. Open Windows Defender en druk op het pijltje naast de knop **Scan uitvoeren**. Kies hier **Volledige scan**. Defender gaat onmiddellijk aan de slag. Hoe je kan reageren wanneer die inderdaad onraad ruikt, lees je in de volgende stap. Zo'n intensieve scanronde kan wel eventjes duren. Het is ook mogelijk om de scan tot een bepaald gebied van je schijf af te bakenen. Selecteer dan **Aangepaste scan** in het uitklapmenu en stip **Scan van geselecteerde stations en mappen** aan. Druk vervolgens op de knop **Selecteren** (zie afbeelding 5). Via de plus-knopjes kan je dan specifieke stations en mappen aanduiden. Bevestig je keuze met **OK** en druk op de knop **Scan nu uitvoeren**.



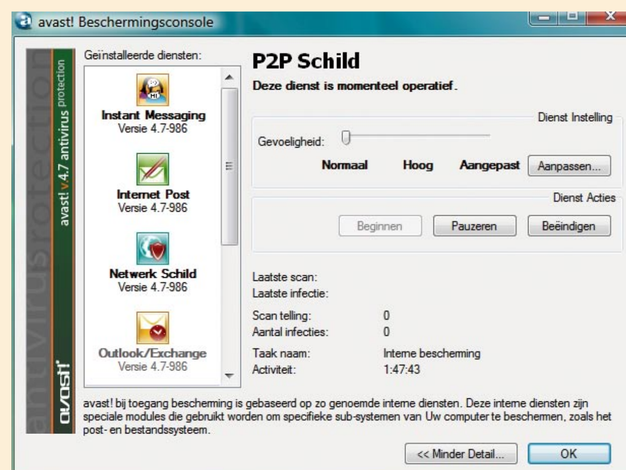
Een scanronde kan je op elk moment zelf van start laten gaan.

STAP 6 / OP ALARM REAGEREN

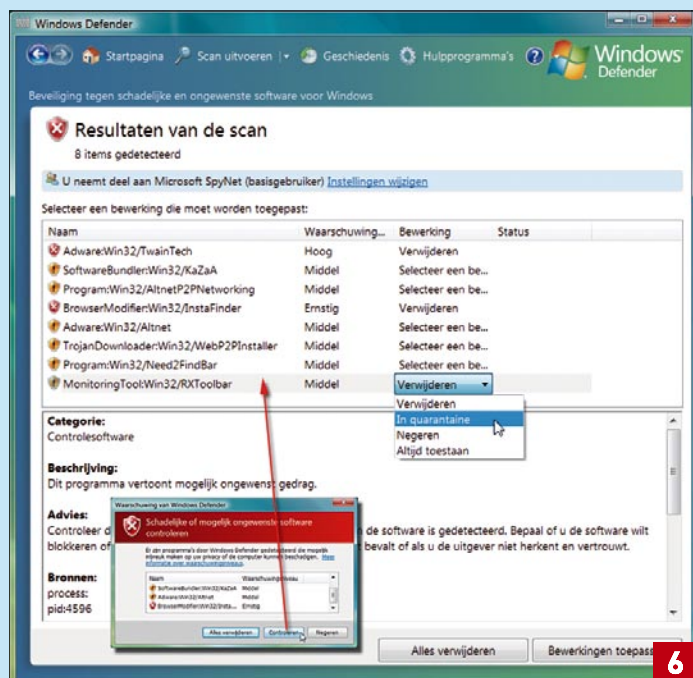
Zodra Windows Defender via de real-time beveiliging of tijdens een scanronde op vermoedelijke malware botst, krijg je daarvan een bericht. We raden je aan telkens eerst op de knop **Controleren** te drukken, of in het hoofdvenster van Defender de link **Items die door real-timebeveiliging / tijdens de scan zijn gedetecteerd, controleren** aan te klikken. Je krijgt nu een overzicht van de verdachte sujetten. Klik die een voor een aan om er meer over te weten te komen. In de kolom **Bewerking** lees je welke actie Defender voorstelt. Met de knop **Verwijderen** haal je de bedreiging meteen van je schijf. Verschijnt **Selecteer een bewerking**, dan kan je zelf de aangewezen actie aanduiden: **Verwijderen**, **Negeren** (dit keer toelaten), **Altijd toestaan** of **In quarantaine** plaatsen. Bevestig je keuzes met **Bewerkingen toepassen**. We raden je aan na zo'n ingreep de pc te herstarten en meteen erna nogmaals een volledige scan te laten uitvoeren. Achteraf kan je zo'n item eventueel nog uit quarantaine halen (zie afbeelding 6). Druk daarvoor op **Hulpprogramma's** en kies **Items in**

VIRUSJAGERS VOOR VISTA

Standaard heeft Vista geen echte antivirustool aan boord. Via de automatische updates krijg je maandelijks wel een vernieuwde versie binnen van het 'Microsoft Windows Hulpprogramma voor verwijderen van schadelijke software'. Dit programma gaat ongemerkt na of je systeem niet besmet is met een of ander virus of worm uit zijn (beperkte) lijst. Zo ja, dan tracht de tool de infectie ongedaan te maken. Je kan altijd nagaan wat de resultaten van elke scanronde waren door met Kladblok het bestand **mrt.log** te openen in de map **%systemroot%\debug**. Je kan de tool trouwens ook zelf downloaden via http://support.microsoft.com/?kbid=890830. Dit tooltje vervangt uiteraard geen echte virusjager die continu zijn werkt doet en infecties tracht te voorkomen! Een gratis antivirusprogramma dat prima onder Vista werkt, is het (ook Nederlandstalige) avast! Home Edition www.avast.nl. Na registratie kan je het programma een jaar gratis gebruiken, waarna je die registratie weer kan verlengen. De tool heeft zich met verschillende 'schilden' gewapend, die niet alleen je surftochten, maar ook je e-mail-, p2p- en chatverkeer monitoren.
Microsoft zelf biedt ook een uitgebreide virusbescherming aan, in de vorm van de all-in service Windows Live OneCare http://onecare.live.com. Na 90 dagen gratis proefdraaien dien je wel met geld over de brug te komen (jaarlijks € 49,95 voor maximaal 3 pc's). Gebruik je antivirussoftware van een andere producent, ga dan na of die inmiddels in een Vista-compatibele versie heeft voorzien, en wat een eventuele upgrade je zal kosten.



Gratis virusbescherming in Vista? Dat kan alvast met avast!

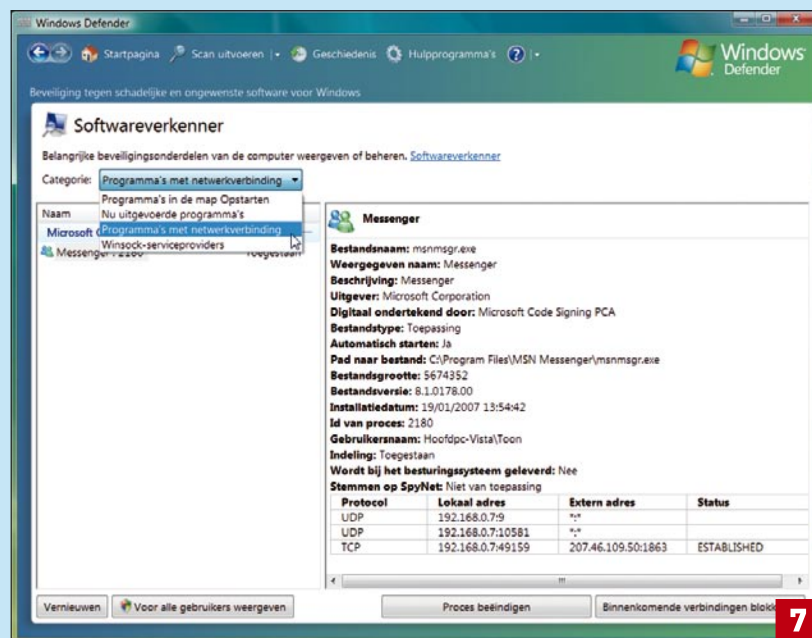


Je kan een verdacht item ook altijd eerst in quarantaine plaatsen, en daarna pas definitief verwijderen.

QUARANTAINE. Selecteer het gewenste item en druk op de knop **HERSTELLEN** – of op **VERWIJDEREN** om het definitief te wissen.

STAP 7 / SOFTWARE 'VERKENNEN'

We mogen ons Defender-verhaal niet afsluiten zonder kennis te maken met de nieuwe **SOFTWAREVERKENNER**, een onderdeel van **HULPPROGRAMMA'S.** Deze tool geeft je namelijk een gedetailleerd overzicht van de programma's die automatisch mee met Vista opstarten. Mee-eters dus, waarvan je sommige misschien liever uitgeschakeld zag. Dat kan! Selecteer het ongewenste item, en druk op **UITSCHAKELEN** of **VERWIJDEREN.** Door bovenaan de **CATEGORIE** te wijzigen in **NU UITGEVOERDE PROGRAMMA'S** krijg je de lijst met software te zien die op dit moment in het geheugen rondhangt. Wil je



Wat roert er zich zoal op je systeem?

een van deze items stopzetten, selecteer het dan en druk op de knop **PROCES BEËINDIGEN.** Hetzelfde kan je doen met items uit de categorie **PROGRAMMA'S MET NETWERKVERBINDING**, hoewel hier **BINNENKOMENDE VERBINDINGEN BLOKKEREN** eveneens een optie is (zie afbeelding 7). Het spreekt echter voor zich dat je met deze softwareverkenner niet zomaar wat moet experimenteren, en willekeurige items moet uitschakelen of verwijderen! ♦

VAKTAAL A - M N - Z

MALWARE: Verzamelnaam voor kwaadaardige software zoals virussen en spyware.

P2P: Peer-to-peer. Twee computers die met elkaar verbonden zijn, zonder andere computers in het netwerk, zijn verbonden via p2p. Veel bestandsuitwisselingsnetwerken, zoals BitTorrent, bedienen zich van deze technologie. Ze gebruiken namelijk geen centrale servers, zodat de data rechtstreeks van de zender naar de ontvanger gaan.